



ENERGY SHIELD

Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

WP7 - COMMUNICATION, DISSEMINATION & ECOSYSTEM DEVELOPMENT

D7.8 – COLLABORATION REPORT

Document info	
Contractual delivery	30/06/2022
Actual delivery	30/06/2022
Responsible Beneficiary	NTUA
Contributing beneficiaries	ALL
Version	1.0



This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907



DOCUMENT INFO

Document ID:	D7.8
Version date:	30/06/2022
Total number of pages:	72
Abstract:	This document summarizes the cross-fertilization activities developed with ongoing EU research and new Horizon 2020 projects focusing on similar challenges with the EnergyShield project and in particular under the BRIDGE initiative. The goal is to leverage the contacts of consortium partners who are involved in other relevant EU research projects, as well as industry associations such as ENTSO-E.
Keywords	Collaboration opportunities, collaboration activities, cross-fertilization activities, synergies.

AUTHORS

Name	Organisation	Role
Anna Georgiadou	NTUA	Overall Editor
Ariadni Michalitsi - Psarrou	NTUA	Overall Editor
Ismail Butun	KTH	Contributor
Otilia Bularca	SIMAVI	Contributor

REVIEWERS

Name	Organisation	Role
Nikola Goranov	CoTTP	Overall Reviewer
Hagai Galili	SIGA	QA Reviewer

VERSION HISTORY

0.1	31/03/2022	Table of contents
0.2	31/05/2022	First version
0.3	09/06/2022	Section 4.7 input from KTH.
0.4	14/06/2022	Section 4 input from SIMAVI.
0.5	14/06/2022	Version ready for overall review.

0.6	15/06/2022	Version ready for QA review.
0.7	27/06/2022	QA review comments.
1.0	30/06/2022	Final version submitted to the EC

EXECUTIVE SUMMARY

This deliverable (D7.8) constitutes EnergyShield's Collaboration Report and contains all information related to any cross-fertilization activities developed with other EU research and new Horizon 2020 projects. Special focus is being made on the BRIDGE initiative as well as any industry associations such as ENTSO-E. This report presents in detail the collaborating projects and initiatives including their goal, field of action and research area, and the contact points used along with the consortium partners who initiated or participated in the collaboration activities. In addition, it sets each collaboration activity's objectives, target audience and desired results and identifies its achieved impact by demonstrating its results.

EnergyShield's collaboration efforts were based on important synergies and project clustering enabling knowledge and experience sharing and exchange among security professionals and experts, academics and researchers, policy making representatives and regulatory parties. Thus, boosting the project results and promoting their communication, dissemination, and exploitation.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
Table of Contents	5
List of figures	6
List of tables	7
Acronyms	8
1 Introduction	9
1.1 Scope and objectives	9
1.2 Structure of the report	9
1.3 Task dependencies	9
2 Collaboration Process	11
3 Collaboration Possibilities	13
4 Collaboration Activities	16
4.1 P2PKOS	16
4.2 BRIDGE	18
4.3 ReachOut	20
4.4 Cyberwatching	21
4.5 SU-DS04-2018-2020	30
4.6 SOCCRATES & HONOR	39
4.7 FLEXIGRID	40
4.8 ECSCI	41
4.9 SPHINX	52
4.10 CyberKit4SME	55
4.11 SPEAR	56
4.12 EnergyShield	57
5 Conclusion	62
6 References	63
7 ANNEXES	64
7.1 Annex A - Collaboration Opportunities EU Survey [ENE19]	64
7.2 Annex B - Collaboration Reports EU Survey [ENE20]	66
7.3 Annex C - Collaboration Opportunities Template	69
7.4 Annex D - Collaboration Reports Template	70

LIST OF FIGURES

Figure 1. Collaboration process.....	11
Figure 2. P2PKOS	17
Figure 3. EnergyShield as part of the BRIDGE initiative.....	19
Figure 4. EnergyShield presence in cyberwatching.eu radar	21
Figure 5. Cyberwatching collaboration activities in chronological order.	21
Figure 6. EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks.....	23
Figure 7. EnergyShield as CyberWatching Project of the Week.	24
Figure 8. Booklet - EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks.....	26
Figure 9. SU-DS04-2018-2020 collaboration activities in chronological order.	31
Figure 10. CYBER-EPES Kick-Off meeting.....	33
Figure 11. ECSCI Projects	42
Figure 12. ECSCI collaboration activities in chronological order.	42
Figure 13. The 2nd ECSCI Workshop on Critical Infrastructure Protection	47
Figure 14. CyberKit4SME collaboration agenda with EnergyShield.....	55
Figure 15. Trends, opportunities and choices in designing a cyber resilient EPES infrastructure.....	58
Figure 16. Building upon cyber resilience in energy sector.....	60

LIST OF TABLES

Table 1. Collaboration Opportunities	13
--	----

ACRONYMS

ACRONYM	DESCRIPTION
D	Deliverable
DoA	Description of Action
M	Month

1 INTRODUCTION

1.1 SCOPE AND OBJECTIVES

The main purpose of this deliverable is to report the collaboration activities held during the EnergyShield project implementation period with other EU research and new Horizon 2020 projects and initiatives.

Collaboration is a fundamental concept in terms of exploiting synergies and driving innovation in research. Therefore, consortium partners who are involved in other EU research projects as well as industry associations, such as ENTSO-E, have identified a list of projects and initiatives focusing on similar challenges to the EnergyShield project.

Having listed several collaboration candidates and studied their goal, field of action and research area, several types of collaboration activities were proposed, materialised and finally reported. Objectives, target audience and achieved results vary depending on the collaboration level, partners involved, and effort invested.

1.2 STRUCTURE OF THE REPORT

This deliverable is structured into three sections:

- The first section presents a comprehensive and flexible collaboration process defined at the beginning of the project.
- The second section briefly lists the collaboration opportunities pinpointed by the consortium partners during the first semester of the project aiming to find an initial exploitable pool of collaboration candidates.
- The third section analyses the collaboration activities, synergies and clustering achieved during the project's lifecycle.

At the end of the deliverable, the following annexes are presented:

- Annex A presents the EU Survey used for informing of collaboration opportunities that are of special interest for the project.
- Annex B presents the EU Survey used for reporting collaboration activities realised.
- Annex C presents the template used for informing of collaboration opportunities that are of special interest for the project.
- Annex D presents the template for reporting collaboration activities realised.

1.3 TASK DEPENDENCIES

T7.4 EU collaboration is closely related to the rest of the WP7 tasks:

- T7.1 - Plan and implement communication activities

- T7.2 - Plan and implement dissemination activities
- T7.3 - Market dissemination and ecosystem development

Our combined approach assisted in better communicating the project's vision, implementation goals, strategies, and practices, therefore, enabling fruitful collaboration activities with other EU projects and initiatives throughout the project's lifecycle. In other words, collaboration was promoted in all phases including designing, implementing, and delivering results.

Since an EU collaboration deliverable was only foreseen at the project's closure, a special collaboration section was included in D7.2 – Communication Report v1, submitted on M12, and its subsequent D7.9 – Communication Report v2, submitted on M24 of the project.

2 COLLABORATION PROCESS

As a starting point, a comprehensive and flexible collaboration process has been defined, presented in Figure 1, consisting of three distinctive steps:

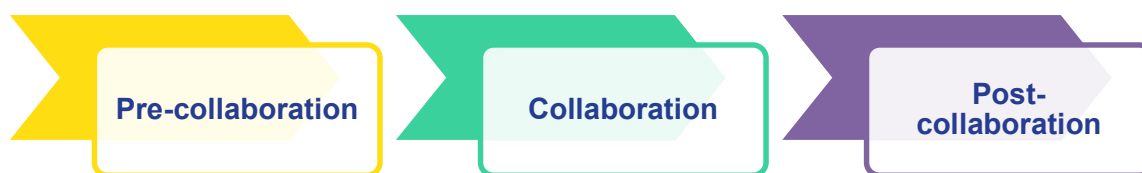


Figure 1. Collaboration process

Pre-collaboration: this step refers to the identification of a new collaboration opportunity and to its reporting via the completion of a collaboration opportunity template. All reports were indexed in a collaboration opportunities repository file, stored in the project file sharing service (Alfresco), and communicated to all consortium partners encouraging creative elaboration, participation and further identification of possible synergies.

To facilitate this step of the collaboration process, two alternatives were made available to the EnergyShield consortium partners:

- an online EU Survey named “**EnergyShield Collaboration Opportunities**” presented in Annex A - Collaboration Opportunities EU Survey [ENE19].
- a collaboration opportunities template file presented in Annex C - Collaboration Opportunities Template.

Collaboration: this step refers to the actual collaboration activity which could be any of the following:

- co-organize or participate to a workshop / event / webinar / hackathon
- share / join forces on social media communication channels / networking boost
- collaboratively work on a publication
- work together towards a common standardization goal
- exchange know-how / expertise / technical documents
- exchange tools / module developed within each project
- collaboration on the development of a tool
- collaboration on evaluation of the tools
- collaboration on the exploitation / marketing of project's assets
- share a framework or toolkit so as to amplify its features
- share data collections and exchange results

Post-collaboration: this step refers to a reporting mechanism. It aimed in collecting data related to the materialised collaboration activity and contributing to post-dissemination and post-communication activities.

To facilitate this step of the collaboration process, two alternatives were made available to the EnergyShield consortium partners (similarly to the pre-collaboration step):

- an online EU Survey named “**EnergyShield Collaboration Reports**” presented in Annex B - Collaboration Reports EU Survey [ENE20]
- a collaboration reports template file presented in Annex D - Collaboration Reports Template

Reports were indexed by updating the corresponding collaboration repository file hosted (as mentioned above) in the project file sharing service (Alfresco).

3 COLLABORATION POSSIBILITIES

During the second semester of the project's life cycle, the consortium partners were asked to report any collaboration opportunities identified in order to initiate a collaboration repository (pre-collaboration step). A number of EU projects and initiatives were put forward constructing a rich collaboration pool. Table 1 briefly presents the information gathered.

Table 1. Collaboration Opportunities

Project/Initiative Suggested	Website	Description
SOCCRATES	https://www.socrates.eu/	SOCCRATES, although it does not focus on the EPES sector, has a similar toolkit setup. The project is bearing a similar life cycle. There are many possibilities of joint activities.
SPHINX	https://sphinx-project.eu/	Exchange know-how and modules of SPHINX Distributed Cyber Situational Awareness Framework & Real Time Risk Assessment.
Infrastructure Resilience - ELVIRA	https://www.his.se/en/research/informatics/distributed-real-time-systems/elvira/	The Elvira project develops time-based infrastructure dependency analysis for the power-grid to model risk assessment and resilience index, which assist decision makers in anticipating failures and their cascading effects.
United Grid	https://united-grid.eu/	The UNITED-GRID project objective is to develop technical solutions to serve needs and opportunities for distribution system operators (DSOs) in their electricity grids.
inteGRIDy	http://integridy.eu/	inteGRIDy aims to integrate cutting-edge technologies, solutions and mechanisms in a Framework of replicable tools to connect existing energy networks with diverse stakeholders, facilitating optimal and dynamic operation of the Distribution Grid (DG), fostering the stability and coordination of distributed energy resources and enabling collaborative storage

		schemes within an increasing share of renewables.
BRIDGE	https://www.h2020-bridge.eu/	BRIDGE is a European Commission initiative which unites Horizon 2020 Smart Grid and Energy Storage Projects to create a structured view of cross-cutting issues which are encountered in the demonstration projects and may constitute an obstacle to innovation. EnergyShield could be part of the proposed working groups and could contribute to the results of the BRIDGE initiative.
FARCROSS	https://farcross.eu/	Present the EnergyShield project targets during the 2020 plenary meeting of FARCROSS which is under the BRIDGE initiative in order to ignite their interest in the project and its results and investigate any possible synergies.
FLEXITRANSTORE	http://www.flexitranstore.eu/	Present the EnergyShield project targets during the 2020 plenary meeting of FLEXITRANSTORE which is under the BRIDGE initiative in order to ignite their interest in the project and its results and investigate any possible synergies.
PHOENIX	https://phoenix-h2020.eu/	Project funded under the SU-DS04-2018-2020 programme and sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).
SDN-microSENSE	https://www.sdnmicrosense.eu/	Project funded under the SU-DS04-2018-2020 programme and sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).
E.DSO-ENCS-ENTSO-E Workshop	https://mailchi.mp/774dd826cbab/edsoencsentso-e-invitation-cybersecurity-workshop-brussels-22-october-2019-still-possible-	The Association of European Distribution System Operators (E.DSO), the European Network for Cyber Security (ENCS) and the European Network of Transmission

	to-register-12439756?e=c3907bfe90	System Operators for Electricity (ENTSO-E) co-organize a Conference on Cybersecurity. The event is scheduled in Brussels on 7 October 2020 and EnergyShield project shall be represented.
ReachOut	https://www.reachout-project.eu/	ReachOut is a Coordination and Support Action (CSA) helping H2020 projects in the area of software technologies to implement beta-testing campaigns. ReachOut act as an operational intermediary between research projects and the open market. ReachOut helps research projects implement beta testing best practices and recruit beta-testers by running promotion initiatives. ReachOut is planning to collaborate with Energyshield for beta-testing tools from the Energyshield toolkit.

Based on this collaboration repository constructed during the first project year and having reached a project and toolkit readiness level suitable for collaborations, partners have initiated a number of collaboration activities with different objectives to communicate the EnergyShield project's goals and progress and investigate possible synergies, as presented in the following section.

4 COLLABORATION ACTIVITIES

EnergyShield's collaboration strategy was based on important synergies founding and leading to various activities such as project clustering, workshops, scientific webinars, publications, tool piloting scenarios and many others as presented in detail in the following sections.

4.1 P2PKOS

Title	"Project to policy kick off seminar" (P2PKOS) for security research
Type	Seminar
Location	REA Convent Garden Building - Brussels
Date	31/01/2020
Description	<p>P2PKOS was organised by the European Commission (Research Executive Agency, DG Migration and Home Affairs and DG Connect). It aimed to raise awareness at 2 levels. On the one hand, projects funded under the Horizon 2020 Societal Challenge 7 call needed to better understand the EU policy landscape in areas such as digital security, protection of critical infrastructure, border management, crime and terrorism or crisis management. On the other hand, EC policy officers working on various security-related areas were interested to get a deeper knowledge of the security research project portfolio and how projects findings could impact and support their policy making work.</p> <p>During a full day of both plenary and group sessions, representatives from H2020 cybersecurity projects, among which EnergyShield partners, shared the objectives of the projects and identified ways they could contribute to the enforcement of European Commission recommendations on cybersecurity in the energy sector – SWD(2019)1240.</p> <p>The possibility to support related initiatives by sharing the recommendations with partners and the EPES value chain via reports and scientific publications was identified.</p>

	<div data-bbox="853 212 997 309" data-label="Image">  </div> <p data-bbox="699 342 1174 454">H2020 – SOCIETAL CHALLENGE 7 "SECURE SOCIETIES" FIRST PROJECT TO POLICY KICK OFF SEMINAR (P2PKOS)</p> <p data-bbox="842 477 927 495">AGENDA</p> <p data-bbox="842 510 1034 595"><i>REA Covent Garden Building COV A2 building - 5th floor Place Rogier 16 Brussels</i></p> <p data-bbox="812 636 1059 667">Figure 2. P2PKOS</p> <p data-bbox="472 689 1402 837">This event was only the start of a process: follow-up actions were defined based on the discussions in order to build a lasting relationship between projects and policy officers for a mutual benefit.</p> <p data-bbox="472 860 1385 891">EnergyShield was introduced among other new H2020 projects:</p> <ul data-bbox="523 913 1402 1066" style="list-style-type: none"> • <u>Digital Security area</u>: EnergyShield, CRITICAL-CHAINS, CyberMar, FORESIGHT, SPIDER, PHOENIX, SOTER, SDN-microSENSE • <u>Infrastructure Protection</u>: SecureGas, InfraStress, SATIE <p data-bbox="472 1088 1402 1160">and actively participated and engaged in all sessions and planned follow-up actions.</p>
Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Link with Horizon 2020 Societal Challenge 7 call projects and policy officers • Build important synergies • Comprehend the EU policy landscape in the areas of digital security and protection of critical infrastructures
Partners Involved	SIMAVI
Type of Audience	<ul style="list-style-type: none"> • Horizon 2020 Societal Challenge 7 call projects • Policy officers
Size of Audience (approx.)	~100 participants
Project/Initiative	<ul style="list-style-type: none"> • 36 project representatives from H2020 cybersecurity projects

Involved	<ul style="list-style-type: none"> • DG Migration and Home Affairs • DG Connect • Research Executive Agency • DG Defence Industry and Space • ECHO • ENER • MARE • MOVE • RTD • TAXUD • JRC • EUROPOL • CEPOL and • FRONTEX
Website	-
Relevant Resources	https://digital-strategy.ec.europa.eu/en/library/project-policy-kick-seminar-security-research

4.2 BRIDGE

Title	BRIDGE General Assembly 2020, 2021, 2022
Type	Workgroup
Location	Brussels
Date	11/02/2020, 02/03/2021, 16/03/2022
Description	<p>The EnergyShield project attended the BRIDGE General Assembly in Brussels on the 11th and 12th of February 2020. As part of this event, the partners introduced the main objectives of the project together while identifying the task forces that could be supported by the project team.</p> <p>EnergyShield Consortium has allocated members in all working groups and is contributing to Action 1 of Data Management - Use case repository.</p>

	 <p>Figure 3. EnergyShield as part of the BRIDGE initiative.</p> <p>In 2021 and 2022, SIMAVI has also attended BRIDGE GAs alongside with the contributing to the Data Management Working Group.</p>
Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Engage with new and old energy sector projects • Network with projects aiming to achieve similar results • Present EnergyShield's challenges in a poster session
Partners Involved	SIMAVI
Type of Audience	Energy sector projects
Size of Audience (approx.)	300 - 500
Project/Initiative Involved	BRIDGE, ETIP Smart Networks for Energy Transition (SNET)
Website	https://www.h2020-bridge.eu/
Relevant Resources	<ul style="list-style-type: none"> • https://www.h2020-bridge.eu/the-2020-bridge-general-assembly-will-take-place-on-february-11th-and-12th-at-the-european-commission/ • https://www.h2020-bridge.eu/event/bridge-general-assembly/

	<ul style="list-style-type: none"> • https://www.h2020-bridge.eu/working-groups/data-management/ • https://bridge-smart-grid-storage-systems-digital-projects.ec.europa.eu/
--	--

4.3 REACHOUT

Title	ReachOut Workshop
Type	Workshop
Location	Online
Date	05/04/2020
Description	The Energyshield and ReachOut projects held a virtual workshop where both projects were presented and discussed. Collaboration ideas were put forward aiming to set up beta-test campaigns for the Energyshield toolkit (starting with the SBA tool and proceeding with the rest of the tools depending on the readiness level).
Dissemination Level	European Union
Activity Objectives	Evaluation of the EnergyShield tools
Partners Involved	NTUA
Type of Audience	-
Size of Audience (approx.)	-
Project/Initiative Involved	ReachOut
Website	https://www.reachout-project.eu/
Relevant Resources	-

4.4 CYBERWATCHING

EnergyShield project was accepted in cyberwatching.eu project hub. In the pre-accession phase, the market and technology readiness were evaluated, and the project was included on the Cybersecurity and Privacy Project Radar.

The Cybersecurity and Privacy Project Radar (<https://radar.cyberwatching.eu/radar>) provides an overview of the complete collection of EU funded projects in the cybersecurity space. Projects have volunteered in a technology and market readiness assessment by Cyberwatching.eu to different degrees.

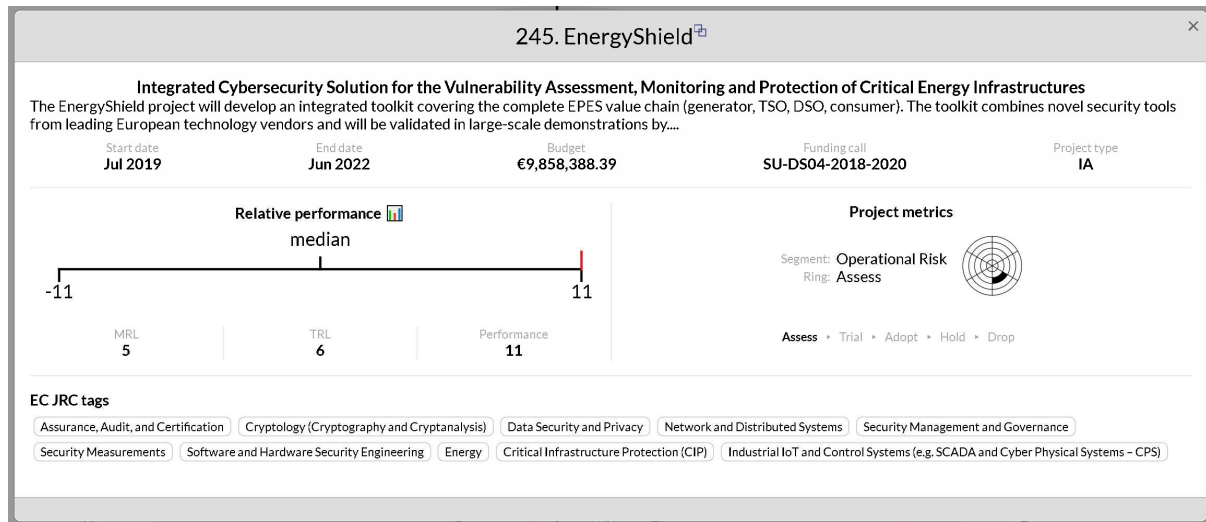


Figure 4. EnergyShield presence in cyberwatching.eu radar

This rather important synergy led to various collaboration activities as presented in Figure 5 and elaborated in detail in the respective tables below.

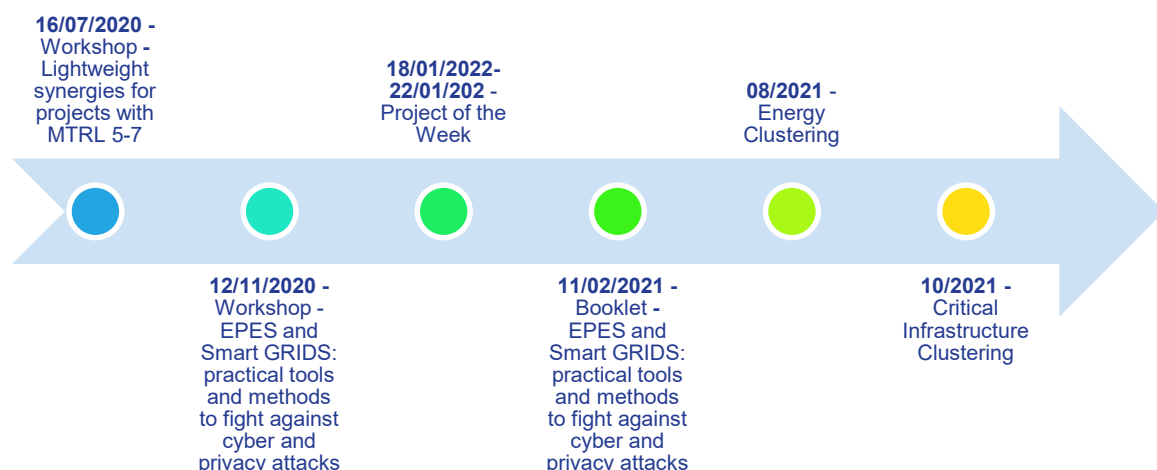


Figure 5. Cyberwatching collaboration activities in chronological order.

Title	Lightweight synergies for projects with MTRL 5-7
Type	Workshop
Location	Online
Date	16/07/2020
Description	<p>CyberWatching, based on projects' responses to their Market and Technology Readiness level questionnaire, identified clustered projects with similar MRL score.</p> <p>The objective of the virtual meeting was to identify possible opportunities for lightweight synergies between projects on activities such as joint webinars, outreach activities.</p> <p>Brief presentations of the participating projects' scope, goals and status were held, among which the EnergyShield project.</p>
Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Identify possible opportunities for lightweight synergies • Network with similar EU projects • Knowledge sharing
Partners Involved	All
Type of Audience	-
Size of Audience (approx.)	~46 participants
Project/Initiative Involved	<ul style="list-style-type: none"> • CyberWatching EU • CS-AWARE • SCOTT • STOP-IT • POSEIDON • THREAT-ARREST • CyberSec4Europe • ECHO • SecureIoT • SECREDAS • InfraStress • CARMEL

Website	https://cyberwatching.eu/
Relevant Resources	-

Title	EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks
Type	Webinar
Location	Online
Date	12/11/2020
Description	<p>Projects EnergySHIELD, SDN-microSENSE, SealedGRID and DEFEND presented their solutions to protect EPES and Smart Grids against cyber-threats and preserve consumers' privacy.</p> <p>EPES AND SMART GRIDS: PRACTICAL TOOLS AND METHODS TO FIGHT AGAINST CYBER AND PRIVACY ATTACKS</p>  <p>Figure 6. EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks.</p>
Dissemination Level	International
Activity Objectives	Present participating project's solutions to existing cyber-security problems met in the EPES sector to interested parties and stakeholders.
Partners	NTUA, KTH, SIMAVI

Involved	
Type of Audience	EPES and Smart Grids' representatives
Size of Audience (approx.)	-
Project/Initiative Involved	<ul style="list-style-type: none"> • CyberWatching • SDN-microSENSE • SealedGRID • DEFEND
Website	https://cyberwatching.eu/
Relevant Resources	https://cyberwatching.eu/epes-and-smart-grids-practical-tools-and-methods-fight-against-cyber-and-privacy-attacks

Title	EnergyShield – CyberWatching Project of the Week
Type	Promotion
Location	Online
Date	18/01/2021 – 22/01/2021
Description	<p>As part of the cyberwatchig.eu hub, EnergyShield was promoted as Project of the Week 18-22 January 2021.</p>  <p>Figure 7. EnergyShield as CyberWatching Project of the Week.</p> <p>Special news items were created and published via different communication channels and social media while EnergyShield's Communication, Dissemination and Collaboration leaders catalysed</p>

	the EnergyShield project mini-site on the Project Hub as an extra channel for visibility by adding News, Events, Videos, etc.
Dissemination Level	International
Activity Objectives	Promote the EnergyShield via different communication and dissemination channels to a broader audience.
Partners Involved	NTUA, KTH, SIMAVI
Type of Audience	-
Size of Audience (approx.)	-
Project/Initiative Involved	CyberWatching
Website	https://cyberwatching.eu/projects/2013/energysield/news-events/integrated-cybersecurity-solution-vulnerability-assessment-monitoring-and-protection-critical-energy-infrastructures
Relevant Resources	<ul style="list-style-type: none"> • https://twitter.com/cyberwatchingeu/status/1352223799178113031 • https://www.linkedin.com/feed/update/urn:li:activity:6757991731976790016

Title	EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks
Type	Booklet
Location	Online
Date	11/02/2021
Description	A post-webinar report presenting concrete recommendations and solutions to protect EPES and Smart Grids against cyber threats and preserve consumers' privacy.

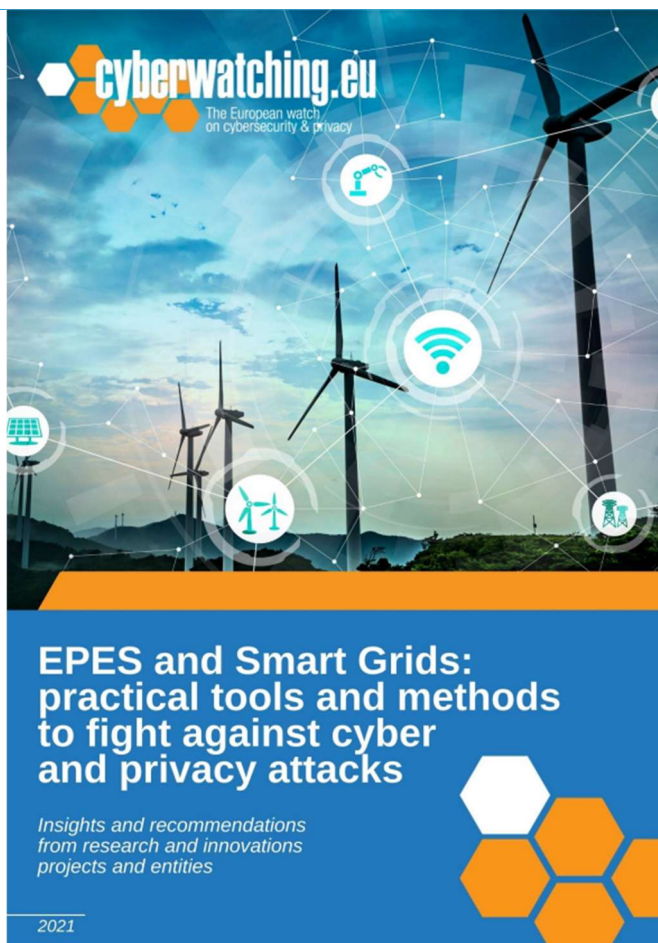


Figure 8. Booklet - EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks.

Dissemination Level	European Union
Activity Objectives	Offer insights and recommendations from the EnergyShield project based on the discussions and presentations made in the “EPES and Smart GRIDS: practical tools and methods to fight against cyber and privacy attacks” webinar.
Partners Involved	NTUA, SIMAVI
Type of Audience	<ul style="list-style-type: none"> • EPES and Smart Grids’ representatives • Security experts and professionals
Size of Audience (approx.)	-
Project/Initiative Involved	<ul style="list-style-type: none"> • SDN-microSENSE • SealedGRID • DEFEND

	<ul style="list-style-type: none"> • CyberWatching
Website	https://cyberwatching.eu/
Relevant Resources	EPES and Smart Grids - practical tools and methods to fight against cyber and privacy attacks.pdf

Title	Energy Clustering
Type	Project Clustering
Location	Online
Date	08/2021
Description	<p>The Energy cluster is focused on cybersecurity applied to the electrical power and energy systems (EPES). EPES, is of key importance to the economy, as all other domains rely on the availability of electricity. Being a sector in deep transformation with digitization, the IoT and the new role of consumers, it is necessary to ensure the proper functioning and resilience of existing infrastructures that can be considered essential, taking into account the installed equipment and legacy systems and analysing how to minimize associated risks. At the same time, the new facilities and equipment that are developed and installed must be done under cybersecurity and privacy principles from the design and throughout the entire supply chain, as well as its life cycle. In this sense, it is essential to define and follow clear standards and a certification framework that provides security to users, manufacturers, and operators. Cybersecurity and its challenges are evolving at a rapid pace, which is why the European Commission has taken a series of measures to tackle it, such as the establishment of a comprehensive legislative framework that builds on:</p> <ul style="list-style-type: none"> • EU Cybersecurity strategy (JOIN 2013)01 final) • Directive on Security of Network and Information Systems (the NIS Directive) (EU) 2016/1148 • Cybersecurity Package (JOIN (2017) 450 final), which also includes the Cybersecurity Act
Dissemination Level	International

Activity Objectives	<ul style="list-style-type: none"> • Increase awareness and preparedness in the energy sector under the guidance of SWD(2019)1240 to implement horizontal cybersecurity rules. • Help transform Europe's energy systems while also maintaining a high level of security, not least in terms of reinforcing cybersecurity of the digital transformation in the energy sector under The Clean Energy for all Europeans packages. • Support Member States' efforts to mandatory include measures on cybersecurity in their national risk assessment plans. • Develop a network code on cybersecurity in the electricity sector. • Raise awareness and promote broad discussions in the energy sector, since cooperation and trust among stakeholders and among the Member States are key when it comes to cybersecurity, due to the potential cascading and cross-border effects. • Exchange best practices between the Member States on identification, mitigation and management of cyber risks under the NIS Directive.
Partners Involved	NTUA, SIMAVI, KTH
Type of Audience	-
Size of Audience (approx.)	-
Project/Initiative Involved	<ul style="list-style-type: none"> • SDN-microSENSE • SealedGRID • DEFEND
Website	https://cyberwatching.eu/
Relevant Resources	https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/energy

Title	Critical Infrastructure Clustering
Type	Project Clustering
Location	Online

Date	10/2021
Description	<p>Critical infrastructure is an asset or system which is essential for providing vital economic and social functions: health, food, security, transport, energy, information systems, financial services, etc. The damage to critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact on the security of the EU and the well-being of its citizens. The concern for cybersecurity lies in giving continuity to the activity and services provided to citizens. Minimal service disruption can have a high impact on an organization and consequently large numbers of people. In turn, the target of cyberattacks has changed. The economic benefit sought by cybercriminals goes to the background, their intentions go far beyond obtaining money through illicit activity, and their ambition is increasing. The current cybercriminal looks for vulnerabilities in critical infrastructure systems in order to obtain relevant information, take control of an activity or an entire organization and what could be worse, paralyze or end the activity. Therefore, security and protection measures become essential in an increasingly complex, interconnected and constantly evolving environment.</p> <p>The projects in this cluster seek to provide solutions to cybersecurity challenges in critical infrastructures, also complying with the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. This initiative is synergistic with ECSCI (European Cluster for Securing Critical Infrastructures), which fosters emerging disruptive solutions for security problems through collaboration and innovation between projects that seek to protect critical infrastructure and services, highlighting the different approaches between grouped projects and establishing close and productive connections with closely related and complementary H2020 projects.</p>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Enhance information security, data privacy, and cybersecurity practice within critical infrastructures. • Encourage organisations to invest, to substitute/upgrade “obsolete” assets, adopting a “security and privacy-by-

	<p>design” approach.</p> <ul style="list-style-type: none"> • Support Member States’ efforts to mandatory include measures on cybersecurity in their national risk assessment plans. • Raise awareness and promote broad discussions in the critical sectors, since cooperation and trust among stakeholders and the Member States are key when it comes to cybersecurity, due to the potential cascading and cross-border effects. • Exchange best practices between the Member States on identification, mitigation and management of cyber risks under the NIS Directive.
Partners Involved	NTUA
Type of Audience	-
Size of Audience (approx.)	-
Project/Initiative Involved	<ul style="list-style-type: none"> • CRITICAL-CHAINS • CYBERSANE • CYBERWISER • FINSEC • INFRASTRESS • PANACEA • ReAct • RESISTO • SDN-microSENSE • STOP-IT
Website	https://cyberwatching.eu/
Relevant Resources	https://cyberwatching.eu/cybersecurity-and-privacy-project-clusters/critical-infrastructure

4.5 SU-DS04-2018-2020

EnergyShield initiated an attempt to bridge the three H2020 EU projects, EnergyShield, PHOENIX and SDN-microSENSE, funded under the SU-DS04-2018-2020 programme and, consequently, sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).

This rather important synergy started with a workshop and led to various dissemination, communication and collaboration activities. The collaboration

roadmap is presented in Figure 9 and elaborated in detail in the respective tables below.





Figure 9. SU-DS04-2018-2020 collaboration activities in chronological order.

SU-DS04-2018-2020 Projects	
Title	SU-DS04-2018-2020 Projects
Type	Workshop
Location	Online
Date	23/07/2020
Description	<p>EnergyShield initiated an attempt to bridge the three H2020 EU projects, EnergyShield, PHOENIX and SDN-microSENSE, funded under the SU-DS04-2018-2020 programme and, consequently, sharing the same goals and vision towards Cybersecurity in the Electrical Power and Energy System (EPES).</p> <p>During the workshop, project representatives shared progress and implementation insights and identified further collaboration opportunities.</p>
Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Bridge the three H2020 EU projects, EnergyShield, PHOENIX and SDN-microSENSE, funded under the SU-DS04-2018-2020 programme • Build an important synergy to function as a starting point for further collaboration activities: <ul style="list-style-type: none"> ◦ Join forces on social media communication channels starting from Twitter ◦ Create a LinkedIn group ◦ Prepare common workshop/conferences involving

	stakeholders <ul style="list-style-type: none"> ○ Publish whitepapers ○ Share costs of booth in events ○ Create a collaboration section on project webpages
Partners Involved	All
Type of Audience	-
Size of Audience (approx.)	~38 participants
Project/Initiative Involved	<ul style="list-style-type: none"> ● PHOENIX ● SDN-microSENSE
Website	<ul style="list-style-type: none"> ● https://phoenix-h2020.eu/ ● https://www.sdnmicrosense.eu/
Relevant Resources	https://energy-shield.eu/3-horizon-epes-project-decide-to-collaborate/

Title	CyberEPES
Type	Clustering
Location	Online
Date	04/06/2021
Description	<p>The major goal of the projects PHOENIX, SDN microSENSE, CyberSEAS, EnergyShield and ELECTRON, all funded by the European Commission/REA under the Digital Security Call “Cybersecurity in the Electrical Power and Energy System (EPES),” is to create an armour against cyber and privacy attacks and data breaches and cybersecure the EPES at European Level. To achieve that goal, all projects design and implement innovative technological platforms and solutions, which are validated in simulated and real Critical Energy Infrastructures and offer controlled dissemination of the results to selected audiences and standardization bodies.</p> <p>In order to maximize the impact of our developments and accelerate the exploitation of the projects' results, these</p>

	<p>projects proceeded in the creation of a Cybersecurity Innovation Cluster for EPES. Though independent, the cluster is supervised by the EC and acts as a think tank and information exchange ecosystem to guide and coordinate the cybersecurity research and innovation results and synchronize the EPES Infrastructure Stakeholders' continuous effort on improving the cybersecurity and resiliency of their infrastructure.</p> <div data-bbox="547 555 1350 674" data-label="Image">  </div> <div data-bbox="643 698 1244 1043" data-label="Image">  </div> <p style="text-align: center;">Cybersecurity Innovation Cluster for EPES Virtual Kick-off Friday 4 June 2021 @ 9:30 CET</p> <p style="text-align: center;">Figure 10. CYBER-EPES Kick-Off meeting.</p> <p>The cluster kick-off virtual event took place on Friday 4 June 2021 with representatives from the Research Executive Agency and European Commission.</p>
Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Maximize the impact of projects (initially PHOENIX, SDN microSENSE, CyberSEAS, EnergyShield and ELECTRON) developments and accelerate the exploitation of the projects' results • The Cluster acts as a think tank and information exchange ecosystem to <ul style="list-style-type: none"> ○ Guide and coordinate the cybersecurity research and innovation results ○ Synchronize the EPES Infrastructure Stakeholders' continuous effort on improving the cybersecurity and resiliency of their infrastructure

	<ul style="list-style-type: none"> ○ Contributing to building the Culture of Security for the wider community/end users via Training/Awareness/Dissemination activities. ● Refine, based on the common project approaches, the coordination of: <ul style="list-style-type: none"> ○ R&D activities ○ Testing activities ○ Policy activities ○ Common events/liaison with relevant stakeholders ○ Define new ones
Partners Involved	SIMAVI
Type of Audience	-
Size of Audience (approx.)	-
Project/Initiative Involved	<ul style="list-style-type: none"> ● PHOENIX ● SDN-microSENSE ● CyberSEAS ● ELECTRON
Website	<ul style="list-style-type: none"> ● https://phoenix-h2020.eu/ ● https://www.sdnmicrosense.eu/ ● https://cyberseas.eu/ ● https://electron-project.eu/
Relevant Resources	https://cyberseas.eu/cyberepes-the-cybersecurity-innovation-cluster-for-epes/

Title	2nd International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2021)
Type	Workshop
Location	Vienna, Austria
Date	17/08/2021 – 20/08/2021
Description	EPESec 2021 workshop was held in conjunction with the 16th International Conference on Availability, Reliability and Security (ARES 2021) . It aimed at collecting the most relevant ongoing research efforts in the EPES digital security field. It also

served as a forum for relevant projects in order to disseminate their security-related results, boost cooperation, knowledge sharing and follow-up synergies, and foster the development of the EPES Security Community, composed of security experts and practitioners.

Topics of interest:

- Security policies
- Risk analysis and management
- Vulnerability assessment and metrics
- Awareness, training and simulation
- Security standards
- Privacy and Anonymity in smart/ micro grids, privacy preserving technologies
- Threat modelling and detection
- Cyber threat intelligence
- Federated machine learning
- Security architectures
- Access control
- Malware and cyber weapons
- Intrusion detection and visualization
- Defense in depth
- Monitoring and real time supervision
- Perimeter security
- Safety-security interactions
- Cyber security engineering
- Secure communication protocols
- Formal models for security (attack trees, indicators of compromise, etc.)
- Hardware Security
- Resilient ICS/CPS
- Application Security
- Secure Firmware
- Incident Response and Digital Forensics
- Incidents and Security Information Sharing
- Countermeasures and Mitigation Actions Recommendation
- Case studies
- Attack simulations
- Penetration testing / ethical hacking in OT and IT
- Data management and interoperability challenges
- EPES market trends and business opportunities

EnergyShield was part of the EPESec 2021 organizing committee, participated in the review process and also contributed with a joint scientific article of two EnergyShield partners, KTH and NTUA:

	<i>Hacks, S., Butun, I., Lagerström, R., Buhaiu, A., Georgiadou, A., & Michalitsi Psarrou, A. (2021, August). Integrating Security Behaviour into Attack Simulations. In The 16th International Conference on Availability, Reliability and Security (pp. 1-13). DOI: 10.1145/3465481.3470475</i>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Present research efforts of the Academic EnergyShield partners • Link with relevant EPES cybersecurity projects • Disseminate project's security-related results • Boost cooperation, knowledge sharing and synergies
Partners Involved	SIMAVI, KTH, KT, NTUA, PSI
Type of Audience	Scientific and Research Community
Size of Audience (approx.)	-
Project/Initiative Involved	<p>The workshop was co-organized by the following H2020 Projects:</p> <ul style="list-style-type: none"> • CYBER-TRUST project: https://cyber-trust.eu/ • EnergyShield https://energy-shield.eu/ • FORESIGHT project: https://foresight-h2020.eu/ • PHOENIX https://phoenix-h2020.eu/ • SDN-microSENSE project: https://www.sdnmicrosense.eu/ • SPEAR https://www.spear2020.eu/
Website	https://www.ares-conference.eu/workshops-eu-symposium/epesec-2021/
Relevant Resources	https://dl.acm.org/doi/proceedings/10.1145/3465481?tocHeading=heading34

Title	3rd International Workshop on Electrical Power and Energy Systems Safety, Security and Resilience (EPESec 2022)
Type	Workshop

Location	Vienna, Austria
Date	23/08/2022 – 26/08/2022
Description	<p>EPESec 2022 workshop will be held in conjunction with the 17th International Conference on Availability, Reliability and Security (ARES 2022). It aims at collecting the most relevant ongoing research efforts in the EPES digital security field. It also serves as a forum for relevant projects in order to disseminate their security-related results, boost cooperation, knowledge sharing and follow-up synergies, and foster the development of the EPES Security Community, composed of security experts and practitioners.</p> <p>Topics of interest:</p> <ul style="list-style-type: none"> • Security policies • Risk analysis and management • Vulnerability assessment and metrics • Awareness, training and simulation • Security standards • Privacy and Anonymity in smart/ micro grids, privacy preserving technologies • Threat modeling and detection • Cyber threat intelligence • Federated machine learning • Security architectures • Access control • Malware and cyber weapons • Intrusion detection and visualization • Defense in depth • Monitoring and real time supervision • Perimeter security • Safety-security interactions • Cyber security engineering • Secure communication protocols • Formal models for security (attack trees, indicators of compromise, etc.) • Hardware Security • Resilient ICS/CPS • Application Security • Secure Firmware • Incident Response and Digital Forensics • Incidents and Security Information Sharing • Countermeasures and Mitigation Actions

	<p>Recommendation</p> <ul style="list-style-type: none"> • Case studies • Attack simulations • Penetration testing / ethical hacking in OT and IT • Data management and interoperability challenges • EPES market trends and business opportunities <p>EnergyShield is part of the EPESec 2022 organizing committee, participated in the review process and has contributed with a scientific article accepted for publication:</p> <p><i>Georgiadou, A., Michalitsi-Psarrou, A. and Askounis, D. Evaluating the Cyber-Security Culture of the EPES Sector. DOI:10.1145/3538969.3543813</i></p>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Present research efforts of the Academic EnergyShield partners • Link with relevant EPES cybersecurity projects • Disseminate project's security-related results • Boost cooperation, knowledge sharing and synergies
Partners Involved	NTUA
Type of Audience	Scientific and Research Community
Size of Audience (approx.)	-
Project/Initiative Involved	<p>The workshop is co-organized by the following H2020 R&D projects which further participate in the CyberEPES Cluster:</p> <ul style="list-style-type: none"> • SDN-microSENSE https://www.sdnmicrosense.eu/ • EnergyShield https://energy-shield.eu/ • PHOENIX https://phoenix-h2020.eu/ • ELECTRON https://electron-project.eu/ • FORESIGHT https://foresight-h2020.eu/
Website	https://www.ares-conference.eu/workshops-eu-symposium/epesec-2022/
Relevant Resources	-

4.6 SOCCRATES & HONOR

Title	powerLang: a probabilistic attack simulation language for the power domain
Type	Joint Publication
Location	Online
Date	25/11/2020
Description	<p>Cyber-attacks on power-related IT and OT infrastructures can have disastrous consequences for individuals, regions, as well as whole nations. In order to respond to these threats, the cyber security assessment of IT and OT infrastructures can foster a higher degree of safety and resilience against cyber-attacks. Therefore, the use of attack simulations based on system architecture models is proposed. To reduce the effort of creating new attack graphs for each system under assessment, domain-specific languages (DSLs) can be employed. DSLs codify the common attack logics of the considered domain.</p> <p>Previously, MAL (the Meta Attack Language) was proposed, which serves as a framework to develop DSLs and generate attack graphs for modelled infrastructures. In this article (DOI: 10.1186/s42162-020-00134-4), powerLang as a MAL-based DSL for modelling IT and OT infrastructures in the power domain is proposed. Further, it allows analysing weaknesses related to known attacks. To comprise powerLang, two existing MAL-based DSL are combined with a new language focusing on industrial control systems (ICS). Finally, this first version of the language was validated against a known cyber-attack.</p> <p>Citation: Hacks, S., Katsikeas, S., Ling, E. et al. powerLang: a probabilistic attack simulation language for the power domain. Energy Inform 3, 30 (2020). https://doi.org/10.1186/s42162-020-00134-4</p>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Present research efforts of the Academic EnergyShield partners • Link with relevant projects on Energy Informatics • Disseminate the project's cybersecurity-related results • Boost cooperation, knowledge sharing and synergies

	among academic peers
Partners Involved	KTH, FOR
Type of Audience	<ul style="list-style-type: none"> Scientific community Cybersecurity professionals and experts
Size of Audience (approx.)	-
Project/Initiative Involved	<ul style="list-style-type: none"> SOCGRATES HONOR
Website	<ul style="list-style-type: none"> https://www.socrates.eu/ https://honor-project.eu/
Relevant Resources	https://link.springer.com/article/10.1186/s42162-020-00134-4

4.7 FLEXIGRID

Title	FLEXIGRID Workshop
Type	Workshop
Location	Online
Date	26/03/2021
Description	<p>FLEXIGRID's T5.3 mentions:</p> <p><i>"Follow the work developed in the projects funded under SU-DS04-2018 call Cybersecurity in Electrical Power and Energy Systems. FLEXIGRID will adopt the solutions that best fit into project particularities."</i></p> <p>After a meeting with the Fundación Circe leading the FLEXIGRID project and a thorough presentation of the EnergyShield toolkit, they came across D2.2 describing the SBA tool and proposed to discuss further the cyber-security culture assessment.</p> <p>During the workshop, the SBA tool was presented in detail while a real-time demo and walk-through of the SaaS version were also held. Possible exploitation scenarios by the</p>

	FLEXIGRID consortium partners and pilots were discussed.
Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Join forces on social media, communication channels / networking boost • Exchange know-how / expertise / technical documents • Exchange tools / module developed within the EnergyShield project.
Partners Involved	NTUA, SIMAVI
Type of Audience	-
Size of Audience (approx.)	~10 participants
Project/Initiative Involved	FLEXGRID
Website	http://www.flexigrid-h2020.eu/
Relevant Resources	-

4.8 ECSCI

EnergyShield reached out to the European Cluster for Securing Critical Infrastructures (ECSCI - <https://www.finsec-project.eu/ecsci>) and joint their effort on **5th May 2021** aiming to participate in the common activities of the ECSCI cluster, such as stakeholders and scientific workshops, joint scientific publications, European common platform for cascading effects on the different critical infrastructures, a platform for combined safety and security for European critical infrastructures, standards and regulations on the protection of critical infrastructures, etc.



Figure 11. ECSCI Projects

This rather important synergy led to various collaboration activities as presented in Figure 12 and elaborated in detail in the respective tables below.

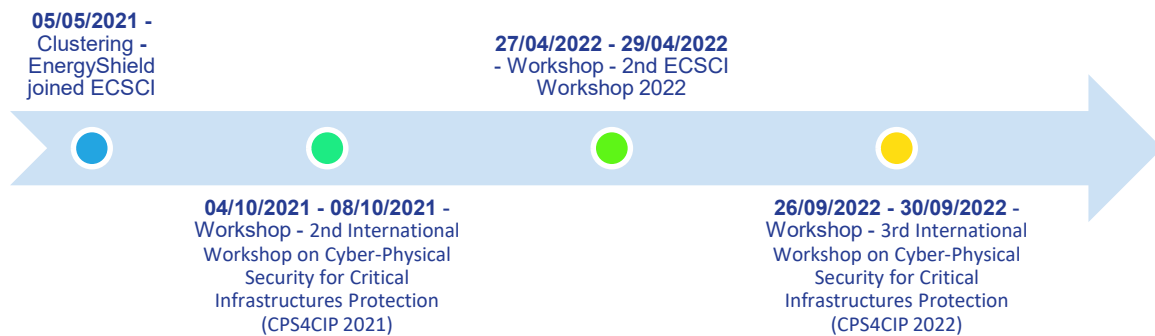


Figure 12. ECSCI collaboration activities in chronological order.

Title	2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021)
Type	Workshop

Location	Online
Date	04/10/2021 – 08/10/2021
Description	<p>The 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021) was co-located with ESORICS 2021.</p> <p>It was the second workshop dedicated to cyber-physical security for protecting critical infrastructures that support finance, energy, health, air transport, communication, gas, and water. The secure operation of these critical infrastructures is essential to the security of a nation, its economy, and the public's health and safety. Security incidents in critical infrastructures can directly lead to a violation of users' safety and privacy, physical damages, significant economic impacts on individuals and companies, and threats to human life while decreasing trust in institutions and questioning their social value. Because of the increasing interconnection between the digital and physical worlds, these infrastructures and services are more critical, sophisticated, and interconnected than ever before. This makes them increasingly vulnerable to attacks, as confirmed by the steady rise of cyber-security incidents, such as phishing or ransomware, but also cyber-physical incidents, such as physical violation of devices or facilities in conjunction with malicious cyber activities.</p> <p>To address all these challenges, the CPS4CIP workshop had the objective of bringing together security researchers and practitioners from the various verticals of critical infrastructures (such as the financial, energy, health, air transport, communication, gas, and water domains) to rethink cyber-physical security in the light of latest technology developments; e.g., Cloud Computing, Blockchain, Big Data, AI, Internet-of-Things (IoT). Specifically, the workshop encouraged contributions focusing on the interplay between the digital and physical aspects of security problems, capable of fostering new, intelligent, collaborative, and more dynamic approaches to detect, prevent and mitigate security incidents, such as:</p> <ul style="list-style-type: none"> • Intelligent monitoring and data collection of security-related information. • Predictive analytics over the collected data based on AI techniques (such as machine learning) that enable the identification of complex attack patterns. • Triggering of preventive and mitigation measures in

	<p>advance of or shortly after the occurrence of an attack.</p> <ul style="list-style-type: none"> • Allowing all stakeholders to collaborate in vulnerability assessment, risk analysis, threat identification, threat mitigation, and compliance. <p>Topics of interest:</p> <ul style="list-style-type: none"> • AI, machine learning for predictive security of critical infrastructures • Integrated (cyber & physical) security • Collaborative risk assessment/mitigation in supply chains • Confronting complex threats and their cascading effects • Adaptive anomaly detection • Blockchain solutions for cyber and data security of critical infrastructures • Risk Assessment and Management • Identification, assessment, and mitigation of cyber-physical threats • Automated vulnerability assessment and penetration testing services • Privacy-preserving data collection and analytics • Dynamic security knowledge base • Measuring Security Levels in critical infrastructures • Adaptive security-related data collection • AI CCTV analytics • Security compliance services • Automation for detection, prevention, and mitigation measures <p>EnergyShield participated in the organizing committee, reviewed scientific articles and held a special presentation in the 3rd session of the workshop unveiling its status, findings and ongoing toolkit trials.</p>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Communicate the project's results, achievements and findings to both the scientific community as well as other EU projects. • Knowledge and experience sharing and exchange. • Promote innovation in research.
Partners Involved	NTUA, KTH, KT

Type of Audience	<ul style="list-style-type: none"> • Critical infrastructure stakeholders • Cybersecurity and Energy professionals and experts • Academia and Research representatives
Size of Audience (approx.)	-
Project/Initiative Involved	<p>The workshop was supported by the projects of the European Cluster for Securing Critical Infrastructures (ECSCI), namely:</p> <ul style="list-style-type: none"> • FINSEC • ANASTACIA • CyberSANE • DEFENDER • ENSURESEC • FeatureCloud • InfraStress • PHOENIX • RESISTO • SAFECARE • SATIE • SecureGas • SmartResilience • SOTER • SPHINX • STOP-IT • 7SHIELD • EnergyShield • IMPETUS • SealedGRID <p>and:</p> <ul style="list-style-type: none"> • NORCICS (Norwegian Center for Cybersecurity in Critical Sectors) project funded by the Research Council of Norway under the Center for Research-based Innovation (SFI) • RESTABILISE4.0 (Restabilise and Energy: Specialization of Enabling Technologies for Balancing Energy Infrastructures and Systems) project Confunded by START4.0 - Competence Center for security and

	optimization of strategic infrastructures
Website	https://st.fbk.eu/events/CPS4CIP2021/
Relevant Resources	<ul style="list-style-type: none"> • https://esorics2021.athene-center.de/ • https://link.springer.com/book/10.1007/978-3-030-88418-5 • https://link.springer.com/book/10.1007/978-3-030-88428-4

Title	2nd ECSCI Workshop
Type	Workshop
Location	Online
Date	27/04/2022 – 29/04/2022
Description	<p>The 2nd ECSCI Workshop presented the different approaches on integrated cyber and physical security in different industrial sectors, such as energy, transport, drinking and wastewater, health, digital infrastructure, banking and financial market, space and public administration. The peculiarities of critical infrastructure protection in each one of these sectors were discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies.</p>

The 2nd ECSCI Workshop on Critical Infrastructure Protection

27th - 29th April 2022



We are pleased to announce that the ECSCI (European Cluster for Securing Critical Infrastructures) will hold its 2nd virtual workshop on April 27-29, 2022!

Within the workshop, interdisciplinary professional communities will be gathered, presenting, discussing and debating on the protection and resilience of critical infrastructures in different domains.

The workshop program includes:

- Remarks from DG Migration and Home Affairs - D2 Counter-Terrorism, DG CNECT Unit H.2 – Cybersecurity and Digital Privacy Policy and DG Migration and Home Affairs, Unit B4 - Innovation and Security Research,
- Keynote speeches from ENISA, JRC and ECSO,
- 24 H2020 projects results presentations,
- Roundtable and panel discussions, and
- Thematic presentations.

Please register and "Save the Date" in your calendars!



[Registration](#)



[2nd ECSCI Workshop](#)



[Agenda](#)

Figure 13. The 2nd ECSCI Workshop on Critical Infrastructure Protection

Specifically, novel techniques were presented for integrated security modelling, IoT security, artificial intelligence for securing critical infrastructures, distributed ledger technologies for security information sharing and increased automation for detection, prevention and mitigation measures.

The workshop included keynote speeches, 23 project presentations, roundtable and panel discussions, and thematic presentations. It foresaw several presentations addressing the following issues:

- Mitigation of combined physical and cyber threats
- New regulatory challenges
- Ethical and legal aspects of security
- Combating Hybrid Threats to Critical Infrastructures
- Cyber and Physical Detection
- Cyber-Physical Security integration and modelling
- Increased automation for detection, prevention and mitigation measures
- Dynamic Safety and Security Risk Assessment
- Information and knowledge sharing environment and respective rules
- Standards, certifications and Regulations on the Protection of Critical Infrastructures
- Common Platform for Cascading Effects on the Different Critical Infrastructures
- Combined Safety and Security for European Critical

	<p>Infrastructures</p> <ul style="list-style-type: none"> • Cyber Security Awareness <p>SIMAVI presented the session “Shielding the power grid from cyberattacks” held during the 1st session of the workshop “The results of EU research on CI protection (part 1)”.</p>
Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Communicate the project’s results, achievements and findings to both the scientific community as well as other EU projects. • Knowledge and experience sharing and exchange. • Promote innovation in research.
Partners Involved	SIMAVI
Type of Audience	<ul style="list-style-type: none"> • Scientists and experts in the field of critical infrastructure protection • CISOs • CIOs • CERTs • CSIRTs • CSOs • Cyber and physical security experts • Policy makers for critical infrastructure protection
Size of Audience (approx.)	-
Project/Initiative Involved	<p>The workshop was supported by the projects of the European Cluster for Securing Critical Infrastructures (ECSCI), namely:</p> <ul style="list-style-type: none"> • FINSEC • ANASTACIA • CyberSANE • DEFENDER • ENSURESEC • FeatureCloud • InfraStress • PHOENIX • RESISTO • SAFE CARE

	<ul style="list-style-type: none"> • SATIE • SecureGas • SmartResilience • SOTER • SPHINX • STOP-IT • 7SHIELD • EnergyShield • IMPETUS • SealedGRID • PRAETORIAN • EU-HYBNET • Precinct • CyberSEAS
Website	https://www.finsec-project.eu/second-ecsci-virtual-workshop
Relevant Resources	https://www.finsec-project.eu/ecsci-2nd-workshop-presentations

Title	3rd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2022)
Type	Workshop
Location	Copenhagen, Denmark
Date	26/09/2022 – 30/09/2022
Description	<p>The 3rd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2022) will be co-located with the 27th European Symposium on Research in Computer Security (ESORICS 2022).</p> <p>CPS4CIP 2022 is the third workshop dedicated to cyber-physical security for protecting critical infrastructures which support finance, energy, health, air transport, communication, gas, and water. The secure operation of such critical environments is essential to the security of a nation, its economy, and public's health and safety. Security incidents in critical infrastructures can directly lead to a violation of users' safety and privacy, physical damages, significant economic</p>

impacts on individuals and companies, and threats to human life, while decreasing trust in institutions and questioning their social value. Because of the increasing interconnection between digital and physical worlds, these infrastructures and services are more critical, sophisticated, and interconnected than ever before. This makes them increasingly vulnerable to attacks, as confirmed by the steady rise of cyber-security incidents, such as phishing or ransomware, but also cyber-physical incidents, such as physical violation of devices or facilities, perpetrated in conjunction with malicious cyber activities.

To address all these challenges, the CPS4CIP workshop has the objective to bring together security researchers and practitioners from the various verticals of critical infrastructures (such as financial, energy, health, air transport, communication, gas and water domains), to rethink cyber-physical security in the light of latest technology developments, e.g., cloud computing, blockchain, big data, AI, Internet of Things (IoT). Specifically, value will be given to contributions focusing on the interplay between the digital and physical aspects of security problems and capable of fostering new, intelligent, collaborative and more dynamic approaches to detect, prevent and mitigate security incidents, such as:

- Intelligent monitoring and data collection of security-related information.
- Predictive analytics over the collected data based on AI techniques (such as machine learning) that enable the identification of complex attack patterns.
- Triggering of preventive and mitigation measures in advance of or shortly after the occurrence of an attack.
- Allowing all stakeholders to collaborate in vulnerability assessment, risk analysis, threat identification, threat mitigation, and compliance.

Topics of interest:

- AI, machine learning for predictive security of critical infrastructures
- Integrated (cyber & physical) security
- Collaborative risk assessment/mitigation in supply chains
- Confronting complex threats and their cascading effects
- Adaptive anomaly detection
- Blockchain solutions for cyber and data security of critical infrastructures

	<ul style="list-style-type: none"> • Risk Assessment and Management • Identification, assessment, and mitigation of cyber-physical threats • Automated vulnerability assessment and penetration testing services • Privacy-preserving data collection and analytics • Dynamic security knowledge base • Measuring Security Levels in critical infrastructures • Adaptive security-related data collection • AI CCTV analytics • Security compliance services • Automation for detection, prevention, and mitigation measures
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Communicate project's results, achievements and findings to both the scientific community as well as other EU projects. • Knowledge and experience sharing and exchange. • Promote innovation in research.
Partners Involved	NTUA
Type of Audience	<ul style="list-style-type: none"> • Critical infrastructure stakeholders • Cybersecurity and Energy professionals and experts • Academia and Research representatives
Size of Audience (approx.)	-
Project/Initiative Involved	<p>The workshop was supported by the projects of the European Cluster for Securing Critical Infrastructures (ECSCI), namely:</p> <ul style="list-style-type: none"> • FINSEC • ANASTACIA • CyberSANE • CyberSEAS • DEFENDER • EnergyShield • ENSURESEC • EU-HYBNET • FeatureCloud • IMPETUS

	<ul style="list-style-type: none"> • InfraStress • PHOENIX • PRAETORIAN • PRECINCT • RESISTO • SAFE CARE • SATIE • SealedGRID • SecureGas • SmartResilience • SOTER • SPHINX • STOP-IT • 7SHIELD <p>and:</p> <ul style="list-style-type: none"> • NORCICS (Norwegian Center for Cybersecurity in Critical Sectors) project funded by the Research Council of Norway under the Center for Research-based Innovation (SFI) • RESTABILISE4.0 (Restabilise and Energy: Specialization of Enabling Technologies for Balancing Energy Infrastructures and Systems) project Confunded by START4.0 - Competence Center for security and optimization of strategic infrastructures
Website	https://st.fbk.eu/events/CPS4CIP2022/
Relevant Resources	-

4.9 SPHINX

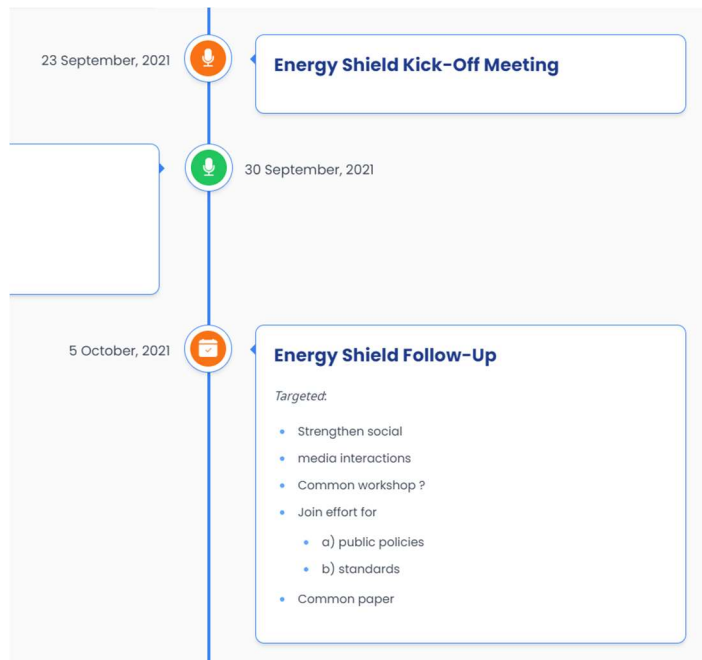
Title	Hospitals' Cybersecurity Culture during the COVID-19 Crisis
Type	Scientific article
Location	Online
Date	07/10/2021
Description	The coronavirus pandemic led to an unprecedented crisis affecting all aspects of the concurrent reality. Its consequences vary from political and societal to technical and economic.

	<p>These side effects provided fertile ground for a noticeable cyber-crime increase targeting critical infrastructures and, more specifically, the health sector; the domain suffering the most during the pandemic. This paper aims to assess the cybersecurity culture readiness of hospitals' workforce during the COVID-19 crisis. Towards that end, a cybersecurity awareness webinar was held in December 2020 targeting Greek Healthcare Institutions. Concepts of cybersecurity policies, standards, best practices, and solutions were addressed. Its effectiveness was evaluated via a two-step procedure. Firstly, an anonymous questionnaire was distributed at the end of the webinar and voluntarily answered by attendees to assess the comprehension level of the presented cybersecurity aspects. Secondly, a post-evaluation phishing campaign was conducted approximately four months after the webinar, addressing non-medical employees. The main goal was to identify security awareness weaknesses and assist in drafting targeted assessment campaigns specifically tailored to the health domain needs. This paper analyses in detail the results of the aforementioned approaches while also outlining the lessons learned along with the future scientific routes deriving from this research.</p>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Apply the SBA tool in another business domain (apart from the Energy sector). • Broaden EnergyShield's application sections.
Partners Involved	NTUA
Type of Audience	<ul style="list-style-type: none"> • Scientific and Research community • Healthcare and security experts
Size of Audience (approx.)	-
Project/Initiative Involved	SPHINX
Website	https://sphinx-project.eu/about-overview/
Relevant Resources	https://doi.org/10.3390/healthcare9101335

Title	A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures
Type	Scientific article
Location	Online
Date	09/02/2022
Description	<p>Recent studies report that cybersecurity breaches noticed in hospitals are associated with low levels of personnel's cybersecurity awareness. This work aims to assess the cybersecurity culture in healthcare institutions from middle- to low-income EU countries. The evaluation process was designed and performed via anonymous online surveys targeting individually ICT (internet and communication technology) departments and healthcare professionals. The study was conducted in 2019 for a health region in Greece, with a significant number of hospitals and health centers, a large hospital in Portugal, and a medical clinic in Romania, with 53.6% and 6.71% response rates for the ICT and healthcare professionals, respectively. Its findings indicate the necessity of establishing individual cybersecurity departments to monitor assets and attitudes while underlying the importance of continuous security awareness training programs. The analysis of our results assists in comprehending the countermeasures, which have been implemented in the healthcare institutions, and consequently enhancing cybersecurity defense, while reducing the risk surface.</p>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Apply the SBA tool in another business domain (apart from the Energy sector). • Broaden EnergyShield's application sections.
Partners Involved	NTUA
Type of Audience	<ul style="list-style-type: none"> • Scientific and Research community • Healthcare and security experts
Size of Audience	-

(approx.)	
Project/Initiative Involved	SPHINX
Website	https://sphinx-project.eu/about-overview/
Relevant Resources	https://doi.org/10.3390/healthcare10020327

4.10 CYBERKIT4SME

Title	CyberKit4SME Workshop
Type	Workshop
Location	Online
Date	05/10/2021
Description	<p>CyberKit4SME EU H2020 Project partners reached out to the EnergyShield looking for cross-project collaboration. An introductory workshop was co-organized where representatives of the two projects presented the goals, objectives, readiness level, achievements and status of the projects.</p>  <p>Figure 14. CyberKit4SME collaboration agenda with EnergyShield.</p>

Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Join forces on social media, communication channels / networking boost • Exchange know-how / expertise / technical documents • Exchange tools / module developed within each project
Partners Involved	NTUA, SIMAVI, KTH
Type of Audience	-
Size of Audience (approx.)	~14 participants
Project/Initiative Involved	CyberKit4SME
Website	https://cyberkit4sme.eu/
Relevant Resources	https://cyberkit4sme.eu/collaboration-h2020/

4.11 SPEAR

Title	SPEAR
Type	Workshop
Location	Online
Date	05/11/2021
Description	<p>One of the pilot partners of the EnergyShield project, VETS, was also participating in the SPEAR project, hosting similar security tools on a workstation serving the project's piloting purposes. A technical workshop was organised and led by NTUA in order to exchange significant information related to the pilot's OT and IT environment. SPEAR representatives shared valuable insights regarding their approach towards the specific pilot, their integration and their results. After the conclusion of the SPEAR project and with the agreement of the pilot partner, specific hardware was offered for co-locating the EnergyShield toolkit.</p>

Dissemination Level	European Union
Activity Objectives	<ul style="list-style-type: none"> • Knowledge sharing regarding the same pilot partner environment • Share data collections and exchange results • Share the same integration environment
Partners Involved	All
Type of Audience	-
Size of Audience (approx.)	~14 participants
Project/Initiative Involved	CyberKit4SME
Website	https://cyberkit4sme.eu/
Relevant Resources	https://cyberkit4sme.eu/collaboration-h2020/

4.12 ENERGYSHIELD

Title	Trends, opportunities and choices in designing a cyber resilient EPES infrastructure
Type	Workshop
Location	Online
Date	15/04/2021
Description	<p>EnergyShield Consortium has organized the European workshop “Trends, opportunities and choices in designing a cyber resilient EPES infrastructure” on the 15th of April 2021, 10.00 CET.</p> <p>The event was initiated and organized by three EnergyShield partners: SIMAVI (Coordinator), KTH (Dissemination & Communication Leader) and NTUA (Collaboration Leader).</p>



Figure 15. Trends, opportunities and choices in designing a cyber resilient EPES infrastructure.

The event gathered Critical Infrastructure stakeholders, business, academia, and industry professionals from 8 European countries around cross-domain topics.

Various aspects of cyber security in the EPES sector including standardization efforts and policy updates were addressed during the opening sessions led by representatives from European Commission, ENISA and energy standardization and regulatory bodies. Also, a brief introduction of the EnergyShield project and a demonstration of the toolkit developed completed this session.

The second part of the workshop focused on two topics that were addressed in two consecutive panels equipped with high profiled experts from the field. The first one elaborated on the effect of work from home on energy and IT infrastructures, while the second one addressed latest incidents targeting critical infrastructure and their impact on designing new technologies, business models and policies.

Dissemination Level

International


Activity Objectives

- Present the EnergyShield project and toolkit to a broader audience
- Bridge critical infrastructure stakeholders, business, academia, and industry professionals
- Explore new collaboration, communication and

	dissemination possibilities.
Partners Involved	All
Type of Audience	<ul style="list-style-type: none"> • Critical infrastructure stakeholders • Cybersecurity and Energy professionals and experts • Academia and Research representatives
Size of Audience (approx.)	135 participants
Project/Initiative Involved	<ul style="list-style-type: none"> • ENISA (European Union Agency for Cybersecurity) • Ofgem (the energy regulator for Great Britain)
Website	-
Relevant Resources	https://energy-shield.eu/registration-open-for-trends-opportunities-and-choices-in-designing-a-cyber-resilient-epes-infrastructure-workshop/ https://energy-shield.eu/energysshield-workshop-report-is-now-out/

As a closure event, the EnergyShield project organised a final workshop where collaboration partners from the different synergies were invited to participate and contribute to the overall discussions related to cyber-security issues in the EPES sector and the results of the project.

Title	Building upon cyber resilience in energy sector
Type	Workshop
Location	Online
Date	23/06/2022
Description	<p>EnergyShield Consortium is organizing the European workshop “Building upon cyber resilience in energy sector” on the 23rd of June 2022, 10.00 CET.</p> <p>The event was initiated and organized by three EnergyShield partners: SIMAVI (Coordinator), KTH (Dissemination & Communication Leader) and NTUA (Collaboration Leader).</p>

	<p>08 Jun 2022 Registration open for EnergyShield's final event online</p> <p>Written by Otilia B Category: Events, News</p> <p>Registrations are now open for EnergyShield's final event online "Building upon cyber resilience in energy sector". Book your seat to the event to receive connection details and updates about the full program.</p> <p>A full day event to present the results of the EnergyShield project and to interact with the audience is prepared by EnergyShield Consortium members.</p> <p>AGENDA (CEST time)</p>  <p>Looking forward to seeing you at the event!</p> <p>Figure 16. Building upon cyber resilience in energy sector.</p> <p>The event aims to communicate the EnergyShield toolkit and its piloting results to Critical Infrastructure stakeholders, business, academia, and industry professionals from different European countries around cross-domain topics.</p> <p>The first session aims to present the overall goals of the project and demonstrate the tools developed and adjusted to the EPES sector during the 3 years of the project lifecycle.</p> <p>The second part of the workshop is targeted in unveiling the application of the toolkit to our EPES pilot partners while elevating the suggested solution as a toolkit suitable for all Critical Infrastructures.</p> <p>ECSCI and CyberEPES representatives shall be joining the presentation and discussions hosted at the end of the workshop.</p>
Dissemination Level	International
Activity Objectives	<ul style="list-style-type: none"> • Present the EnergyShield project and toolkit to a broader audience • Bridge critical infrastructure stakeholders, business, academia, and industry professionals • Demonstrate results of collaboration, communication and dissemination activities.
Partners Involved	All
Type of Audience	<ul style="list-style-type: none"> • Critical infrastructure stakeholders • Cybersecurity and Energy professionals and experts • Academia and Research representatives

Size of Audience (approx.)	-
Project/Initiative Involved	<ul style="list-style-type: none"> • European Cluster for Securing Critical Infrastructures (ECSCI) • CyberEPES
Website	-
Relevant Resources	<ul style="list-style-type: none"> • https://energy-shield.eu/registration-open-for-energyshields-final-event-online/ • https://ec.europa.eu/eusurvey/runner/e64c7227-e5bd-dafe-85c1-bc0401516303 • https://twitter.com/EnergyShield/status/1534466556729643008

5 CONCLUSION

This deliverable presented the collaboration strategy, methodology, approach and achievements during the EnergyShield project implementation period involving other EU research and new Horizon 2020 projects and initiatives.

Based on a carefully designed methodology with simplified and distinctive steps, the consortium partners were facilitated in collaboratively exploring the EU research and innovation community, the cyber-security landscape, authorities and professionals and the international concurrent reality.

The coronavirus pandemic led to an unprecedented crisis in many different aspects of the concurrent reality along with an unforeseen cyber-crime increase. Cyber-security solutions gained focus and ground on this basis, among which is the EnergyShield toolkit. A combined and well-elaborated communication, dissemination, collaboration and exploitation plan led to the promotion of the project's tools and overall solution to a broader audience expanding further than the Energy sector.

EnergyShield will continue to support cluster activities, sharing knowledge, and disseminating its results for their exploitation in similar, future projects.

6 REFERENCES

- [ENE19] EnergyShield Collaboration Opportunities. National Technical University of Athens. Available online: <https://ec.europa.eu/eusurvey/runner/EnergyShieldCollaborationOpportunitiesv2> (Accessed on 25 May 2022).
- [ENE20] EnergyShield Collaboration Reports. National Technical University of Athens. Available online: <https://ec.europa.eu/eusurvey/runner/EnergyShieldCollaborationReports> (Accessed on 25 May 2022).

7 ANNEXES

7.1 ANNEX A - COLLABORATION OPPORTUNITIES EU SURVEY [\[ENE19\]](#)

EnergyShield Collaboration Opportunities

Fields marked with * are mandatory.



EnergyShield Collaboration Opportunities Survey

This questionnaire should be used by all EnergyShield partners to inform of collaboration opportunities that are of special interest for the project.

*Full Name of the person recommending the collaboration activity

It shall also be used as a contact point when collaboration opportunity is being exploited.

*EnergyShield Partner

*Email Address

*Project/Initiative Suggested

Website

Related to the suggested project/initiative, if it exists.

Title of collaboration activity**Type of collaboration activity**

- ☐ co-organize or participate to a workshop / event / webinar / hackathon
- ☐ share / join forces on social media communication channels / networking boost
- ☐ collaboratively work on a publication
- ☐ work together towards a common standardization goal
- ☐ exchange know-how / expertise / technical documents
- ☐ exchange tools / module developed within each project
- ☐ collaboration on the development of a tool
- ☐ collaboration on evaluation of the tools
- ☐ collaboration on the exploitation / marketing of project's assets
- ☐ share a framework or toolkit so as to amplify its features
- ☐ share data collections and exchange results
- ☐ other

Other type of collaboration activity

In case you have selected "other" in previous field, please further describe.

***Description**

7.2 ANNEX B - COLLABORATION REPORTS EU SURVEY [\[ENE20\]](#)

EnergyShield Collaboration Reports

Fields marked with * are mandatory.



EnergyShield Collaboration Activities Report

This questionnaire should be used by all EnergyShield partners to report all collaboration activities realised.

***Full Name of the person reporting the collaboration activity**

It shall also be used as a contact point for extra information regarding the collaboration activity.

***EnergyShield Partner**

***Email Address**

***Project/Initiative Involved**

Website

Related to the involved project/initiative, if it exists.

*** Title of collaboration activity***** Type of collaboration activity**

- ☐ co-organize or participate to a workshop / event / webinar / hackathon
- ☐ share / join forces on social media communication channels / networking boost
- ☐ collaboratively work on a publication
- ☐ work together towards a common standardization goal
- ☐ exchange know-how / expertise / technical documents
- ☐ exchange tools / module developed within each project
- ☐ collaboration on the development of a tool
- ☐ collaboration on evaluation of the tools
- ☐ collaboration on the exploitation / marketing of project's assets
- ☐ share a framework or toolkit so as to amplify its features
- ☐ share data collections and exchange results
- ☐ other

Other type of collaboration activity

In case you have selected "other" in previous field, please further describe.

Location**Date**

*** Description***** Dissemination Level**

- ☐ National
- ☐ Regional
- ☐ European Union
- ☐ Global

Activity Objectives*** Partners Involved***** Type of audience***** Size of audience (approx.)****Relevant Resources**

The maximum file size is 1 MB

Select file to upload

7.3 ANNEX C - COLLABORATION OPPORTUNITIES TEMPLATE

Title	The title of the collaboration activity
Type	<p>The type of the collaboration activity:</p> <ul style="list-style-type: none"> • co-organize or participate to a workshop / event / webinar / hackathon • share / join forces on social media communication channels / networking boost • collaboratively work on a publication • work together towards a common standardization goal • exchange know-how / expertise / technical documents • exchange tools / module developed within each project • collaboration on the development of a tool • collaboration on evaluation of the tools • collaboration on the exploitation / marketing of project's assets • share a framework or toolkit so as to amplify its features • share data collections and exchange results • other: <div style="border: 1px solid black; height: 20px; width: 300px; margin-top: 5px;"></div>
Description	A brief description of the proposed collaboration activity.
Project/Initiative Suggested	The EU research / Horizon 2020 project OR initiative suggested to collaborate with.
Website	A website related to the suggested project/initiative, if it exists.

7.4 ANNEX D - COLLABORATION REPORTS TEMPLATE

Title	The title of the collaboration activity
Type	<p>The type of the collaboration activity:</p> <ul style="list-style-type: none"> • co-organize or participate to a workshop / event / webinar / hackathon • share / join forces on social media communication channels / networking boost • collaboratively work on a publication • work together towards a common standardization goal • exchange know-how / expertise / technical documents • exchange tools / module developed within each project • collaboration on the development of a tool • collaboration on evaluation of the tools • collaboration on the exploitation / marketing of project's assets • share a framework or toolkit so as to amplify its features • share data collections and exchange results • other: <div style="border: 1px solid black; height: 20px; width: 300px; margin-top: 5px;"></div>
Location	The location that the collaboration activity took place (if applicable).
Date	The date that the collaboration activity took place.
Description	A brief description of the collaboration activity (~ 5 lines).
Dissemination Level	<ul style="list-style-type: none"> • National • Regional • European Union • Global
Activity Objectives	The objectives of the collaboration activity.
Partners Involved	The EnergyShield partners involved in the collaboration activity.

Type of Audience	<p>The type of the audience could be one of the following:</p> <ul style="list-style-type: none"> • Cybersecurity vendors • Cybersecurity consultancies • Critical Infrastructure operators • Cybersecurity researchers • Social scientists • ENISA • CERT-EU • Media • Consumers • Other: <div data-bbox="719 723 1201 775" style="border: 1px solid black; height: 23px; width: 302px; margin-left: 350px;"></div>
Size of Audience (approx.)	
Project/Initiative Involved	The EU research / Horizon 2020 project OR initiative involved in collaboration.
Website	A website related to the suggested project/initiative, if it exists.
Relevant Resources	<p>Files such as:</p> <ul style="list-style-type: none"> • Brochures • Presentations • Journal Articles • URLs • etc.

DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID



www.energy-shield.eu

